UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia

UNDER SEAL

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
Information Associated With Email Account [redacted]@Gmail.com That Is Stored At Premises Controlled By Google, Inc.

Case No. 1:16-SW- 331

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Northern District of California
(identify the person or describe the property to be searched and give its location):

See Attachment A

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*:

See Attachment B

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before July 4, 2016
(not to exceed 14 days)

☑ in the daytime 6:00 a.m. to 10 p.m. ☐ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge Michael S. Nachmanoff.
(name)

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)* ☐ for _____ days *(not to exceed 30)*.

☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 6/20/16 @3:31pm

/s/
Michael S. Nachmanoff
United States Magistrate Judge
Judge's signature

City and state: Alexandria, Virginia

Michael S. Nachmanoff, United States Magistrate Judge
Printed name and title

UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia

FILED UNDER SEAL

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
Information Associated With Email Account [redacted]@Gmail.com That Is Stored At Premises Controlled By Google, Inc.

Case No. 1:16-SW-337

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. 793(e);	Unlawful possession and communication of national defense information (NDI);
18 U.S.C. 793(f)	Unlawful removal or failure to report unlawful removal of NDI

The application is based on these facts:

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

[redacted]
Applicant's signature

[redacted], Special Agent, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: 06/20/2016

/s/
Michael S. Nachmanoff
United States Magistrate Judge
Judge's signature

City and state: Alexandria, Virginia

Michael S. Nachmanoff, United States Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

Alexandria Division

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH EMAIL ACCOUNT [redacted]@GMAIL.COM THAT IS STORED AT PREMISES CONTROLLED BY GOOGLE, INC.	))))))	**UNDER SEAL** Case No. 1:16-331

AFFIDAVIT IN SUPPORT OF A SEARCH AND SEIZURE WARRANT

I, [redacted], being duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. The government is conducting a criminal investigation concerning the improper transmission and storage of classified information on unclassified email systems and servers. The investigation began as a result of a review of emails undertaken by the U.S. Department of State (State Department) in connection with Freedom of Information Act (FOIA) litigation. During this FOIA review, it was determined that certain emails containing classified information were sent and received on systems unauthorized for the transmission or storage of such information. On or about July 6, 2015, the Inspector General for the Intelligence Community notified the Federal Bureau of Investigation (FBI) of a potential compromise of classified information involving the emails discovered through the FOIA review. After an initial review of the matter, the FBI opened a criminal investigation to, among other things, identify any unauthorized systems which the emails in question have transited, identify any person(s) who may have introduced classified information onto unauthorized systems and all circumstances surrounding such introduction, identify any person(s) who may have transmitted information

over any such systems, and identify whether classified information has been compromised through computer intrusions or unauthorized access into these systems.

2. The FBI's investigation has established that emails containing classified information have been transmitted and stored on multiple forms of electronic media. One of the items identified as having contained such emails is a server which was used by former Secretary of State Hillary Rodham Clinton (Clinton) to transmit, receive, and store email for a personal email account or accounts she maintained. One domain on that server used by Clinton was @clintonemail.com.

3. The purpose of this affidavit is to secure a search and seizure warrant for the Google account [redacted] which is associated with the email address [redacted]@gmail.com (hereinafter the "SUBJECT ACCOUNT"), within the possession and control of the remote computing service and electronic communication service provider, also referred to as an Internet Service Provider or "ISP," known as Google, Inc. (Google), more fully described in Attachment A. There is probable cause to believe that the SUBJECT ACCOUNT contains evidence, contraband, fruits and/or other items illegally possessed in violation of 18 U.S.C. § 793(e) and (f).

4. The search warrant is sought under 18 U.S.C. § 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require Google to disclose to the government records and other information in their possession, pertaining to the subscriber(s) or customer(s) associated with the SUBJECT ACCOUNT, including contents of electronic communications.

5. I am a Special Agent with the FBI, and have been since June 1998. As a Special Agent, I have been assigned to the Criminal, Counterterrorism, and Counterintelligence Divisions of the FBI's Washington Field Office. From 2010 to 2015, I served as a Supervisory

Special Agent in the International Operations Division at FBI Headquarters and in Milan, Italy, where I supported Counterintelligence operations. In January 2015, I was assigned to the Counterintelligence Division in the Washington Field Office as a Supervisory Special Agent responsible for investigating offenses involving espionage, illegal agents of foreign powers, United States trade sanctions, unauthorized retention and disclosure of classified and national defense information, and money laundering in furtherance of national security offenses.

SOURCE OF EVIDENCE

6. The facts set forth in this affidavit are based on my personal knowledge, knowledge obtained during my participation in this investigation, and information from other FBI and U.S. Government personnel. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation.

STATUTORY AUTHORITY AND DEFINITIONS

7. Under 18 U.S.C. § 793(e), "[w]hoever having unauthorized possession of, access to, or control over any document . . . or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted" or attempts to do or causes the same "to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it" shall be fined or imprisoned not more than ten years, or both.

8. Under 18 U.S.C. § 793(f), "[w]hoever, being entrusted with or having lawful possession or control of any document . . . or information, relating to the national defense" either

"(1) through gross negligence permits the same to be removed from its proper place of custody or delivered to anyone in violation of his trust, or to be lost, stolen, abstracted, or destroyed," or "(2) having knowledge that the same has been illegally removed from its proper place of custody or delivered to anyone in violation of its trust, or lost, or stolen, abstracted, or destroyed, and fails to make prompt report of such loss, theft, abstraction, or destruction to his superior officer" shall be fined or imprisoned not more than ten years, or both.

9. Under Executive Order 13526, information in any form may be classified if it: (1) is owned by, produced by or for, or is under the control of the United States government; (2) falls within one or more of the categories set forth in the Executive Order [Top Secret, Secret, and Confidential]; and (3) is classified by an original classification authority who determines that its unauthorized disclosure reasonably could be expected to result in damage to the national security.

10. Where such unauthorized disclosure could reasonably result in damage to the national security, the information may be classified as "Confidential" and must be properly safeguarded. Where such unauthorized disclosure could reasonably result in serious damage to the national security, the information may be classified as "Secret" and must be properly safeguarded. Where such unauthorized disclosure could reasonably result in exceptionally grave damage to the national security, the information may be classified as "Top Secret" and must be properly safeguarded.

11. Sensitive Compartmented Information (SCI) means classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems.

12. Classified information, of any designation, may be shared only with persons

determined by an appropriate United States government official to be eligible for access, and who possess a "need to know." Among other requirements, in order for a person to obtain a security clearance allowing that person access to classified United States government information, that person is required to and must agree to properly protect classified information by not disclosing such information to persons not entitled to receive it, by not unlawfully removing classified information from authorized storage facilities, and by not storing classified information in unauthorized locations. If a person is not eligible to receive classified information, classified information may not be disclosed to that person. In order for a foreign government to receive access to classified information, the originating United States agency must determine that such release is appropriate.

13. Pursuant to Executive Order 13526, classified information contained on automated information systems, including networks and telecommunications systems, that collect, create, communicate, compute, disseminate, process, or store classified information must be maintained in a manner that: (1) prevents access by unauthorized persons; and (2) ensures the integrity of the information.

14. 32 C.F.R. Parts 2001 and 2003 regulate the handling of classified information. Specifically, 32 C.F.R. § 2001.43, titled "Storage," regulates the physical protection of classified information. This section prescribes that Secret and Top Secret information "shall be stored in a GSA-approved security container, a vault built to Federal Standard (FED STD) 832, or an open storage area constructed in accordance with § 2001.53." It also requires periodic inspection of the container and the use of an Intrusion Detection System, among other things.

PROBABLE CAUSE FOR SEARCH

15. Clinton served as the Secretary of State from on or about January 21, 2009 to on or about February 1, 2013. On or about March 9, 2009, Clinton began using a private email server (Server 1) to transmit, receive, and store email for a personal email account she maintained. One domain on Server 1 was @clintonemail.com. From March 2009 to June 2013, Server 1 was housed at Clinton's residence in Chappaqua, New York.

16. In June 2013, Clinton retained Platte River Networks (PRN), a Denver, Colorado-based information technology firm, to establish and administer a new email server (Server 2) to replace Server 1. On or about June 22, 2013, PRN installed and set up Server 2 at Equinix, a datacenter located in Secaucus, New Jersey. Based upon interviews and a review of the business records produced by PRN pursuant to a grand jury subpoena, the FBI determined that shortly after PRN took control of Server 1 in June 2013, PRN transferred all email accounts and associated data from Server 1 to Server 2. Server 1 and Server 2, regardless of their physical location(s), were not devices authorized by the United States government to store or transmit classified or national defense information.

17. Based upon a records request, Clinton produced to the State Department approximately 30,490 email communications sent to or from Clinton at the @clintonemail.com domain that resided on Server 1 and Server 2. As a result of a FOIA request, the State Department ultimately reviewed these 30,490 emails. The FOIA process implemented by the State Department required that these emails be reviewed by government agencies for classified information prior to public release. In February 2016, the State Department completed its review and determined that 2,115 of the 30,490 emails contain information that is presently classified.

18. The State Department released 2,093 of the emails containing classified

information to the public in redacted form beginning in May 2015 and ending in February 2016. According to the relevant original classification authorities, 2,028 contained information classified as Confidential and 65 contained information classified as Secret. In addition, the State Department determined that 22 emails containing information classified at the Top Secret level, as determined by the relevant original classification authorities, would be withheld in their entirety from public release.

19. The U.S. Government's determination that 2,028 emails contain information classified at the Confidential level is significant because it means that the unauthorized disclosure of those emails could result in damage to national security. The U.S. Government's determination that 65 emails contain information classified at the Secret level is significant because it means that the unauthorized disclosure of those emails could result in serious damage to national security. The U.S. Government's determination that 22 emails contain information classified at the Top Secret level is significant because it means that the unauthorized disclosure of those emails could result in exceptionally grave damage to national security.

20. In or about July 2015, the FBI initiated a criminal investigation into the possible mishandling and compromise of national security information from unauthorized electronic communications systems. As part of the investigation, the FBI has obtained private server equipment and related devices used by Clinton and her staff during her tenure as Secretary of State. The FBI's review of this material identified emails that were later determined by the relevant original classification authorities to contain information classified up to the Top Secret/Sensitive Compartmented Information level.

21. Clinton's personal counsel for purposes of the present investigation, Williams & Connolly LLP, provided written consent to the Department of Justice for the FBI to obtain

Server 1 and Server 2 as well as physical and electronic copies of the 30,490 emails that Clinton, through her counsel, had previously provided to the State Department.

22. Pursuant to the FBI's review of the 30,490 @clintonemail.com emails described above, the FBI determined that a large portion of the emails contained metadata displaying the SUBJECT ACCOUNT. According to subpoena returns from Google, the SUBJECT ACCOUNT is associated with PRN employee Paul Combetta.

23. In a recent interview, Combetta informed the FBI that he used the SUBJECT ACCOUNT to facilitate the transfer of archived Clinton emails to Server 2 from a laptop belonging to a former State Department employee who worked on Clinton's staff. The FBI believes these archived emails included emails from the original set provided to the State Department --- and subsequently to the FBI --- by Williams & Connolly. As noted above, these emails include information that has since been determined to be classified.

24. Based upon an order obtained pursuant to 18 U.S.C. § 2703(d), the FBI determined that 820 @clintonemail.com emails, dated within the time frame October 25, 2010 to December 31, 2010, are currently present in the SUBJECT ACCOUNT. Out of the 820 emails, the FBI identified 57 emails that have been determined by the relevant original classification authorities to contain information currently classified at the Confidential level. The FBI has confirmed that at least one of the 57 emails contained information that, although not marked as such, was classified at the Secret level at the time the email was sent. The original classification authorities did not make a determination as to whether the information in the remaining 56 emails was classified at the time that the emails were sent to or from Clinton at the @clintonemail.com domain. As part of its investigation, the FBI has sought a determination by the relevant original classification authorities as to whether these emails contained classified

information at the time they were sent. That request is currently pending.

25. I have probable cause to believe that the SUBJECT ACCOUNT contains information classified at the Confidential level, which was produced by and is owned by the U.S. Government. Such information is being stored in an unauthorized location and in an unauthorized manner. Accordingly, I am seeking the issuance of a warrant to search the SUBJECT ACCOUNT for items described in Attachment B.

BACKGROUND ON EMAIL

26. In my training and experience and based on information obtained from other law enforcement officers, I understand the following about email providers, such as Google:

a. Google provides a variety of on-line services, including email access, to the public. Google allows subscribers to obtain email accounts at the domain name gmail.com. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information.

b. In addition to the account, subscriber, and IP address login/logout (session) information, which can assist in identifying who controls/uses the account and which computers or other devices were used to access the account (and when such access occurred), the computers of Google are likely to contain stored electronic communications (including retrieved and unretrieved email).

c. A Google subscriber can also store address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Google. In my training and experience, evidence of who was using an email account may be found in address books,

contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

d. In some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. Such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

27. A subscriber may store email, for example, on Google servers for which there is insufficient storage space in the subscriber's computer or which he does not wish to maintain on his own computer. A search of the email on a subscriber's "home" computer will not necessarily uncover the files, messages, and other information maintained by a subscriber on Google servers.

SEARCH PROCEDURE

28. This warrant will be executed in compliance with ECPA. Specifically, the warrant will require Google to disclose to the government a copy of the records and other information (including the content of communications, if any) described in Part I of Attachment B. Upon receipt of such information, the information described in Part III of Attachment B will be subject to search by law enforcement.

29. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. See 18 U.S.C. § 2703(a), (b)(1)(A),

(c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

30. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

CONCLUSION

Based on the foregoing facts and circumstances, I submit that probable cause exists to believe that evidence, contraband, fruits and/or other items illegally possessed in violation of 18 U.S.C. § 793(e) and (f) are located in the SUBJECT ACCOUNT. Accordingly, I seek the issuance of a warrant to search the SUBJECT ACCOUNT for evidence, contraband, fruits, and/or other items illegally possessed (more particularly described in Attachment B), in violation of 18 U.S.C. § 793(e) and (f).

[redacted]
Supervisory Special Agent
Federal Bureau of Investigation

Sworn to and subscribed before me this 21st day of June, 2016.

/s/
Michael S. Nachmanoff
United States Magistrate Judge

Michael S. Nachmanoff
United States Magistrate Judge

ATTACHMENT A

Property To Be Searched

This warrant applies to information associated with Google account [redacted], which is associated with the email address [redacted]@gmail.com ("SUBJECT ACCOUNT") that is stored at premises controlled by Google Inc., a company that does business and accepts process at 1600 Amphitheater Parkway, Mountain View, California 94043.

ATTACHMENT B

Particular Things To Be Seized

I. Information To Be Disclosed by Google

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, including any emails, records, files, logs, or information that has been deleted but is still available to Google, or has been preserved pursuant to requests made under 18 U.S.C. § 2703(f) on February 22, 2015 and June 3, 2016, Google is required to disclose the following information to the government for the SUBJECT ACCOUNT:

a. The contents of all emails associated with the SUBJECT ACCOUNT, including stored or preserved copies of emails sent to and from the SUBJECT ACCOUNT, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the SUBJECT ACCOUNT, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored at any time by an individual using the SUBJECT ACCOUNT, including address books, contact and buddy lists, calendar data, pictures, and files; and

e. All records pertaining to communications between Google and any person regarding the SUBJECT ACCOUNT, including contacts with support services and records of actions taken.

II. Key Word Searches

Law enforcement personnel will search the contents of email communications, for the time period October 25, 2010 to December 31, 2010, provided by Google to identify emails meeting the following criteria, which will be the emails reviewed pursuant to this search warrant:

a. Any email communications sent by the SUBJECT ACCOUNT to a .gov email address or sent to the SUBJECT ACCOUNT from a .gov email address, as well as any emails to or from the SUBJECT ACCOUNT on which a .gov email address was carbon copied or blind carbon copied;

b. Any email communications sent to or from the SUBJECT ACCOUNT containing prior emails from, to, or carbon copying a .gov email address;

c. Any email communications sent to or from the SUBJECT ACCOUNT containing prior emails from, to, or carbon copying a @clintonemail.com email address;

d. Any email communications that contain any of the key words from a list of terms used by the FBI in this case. The FBI has developed a list of terms to include key words utilized to locate emails and files related to the improper transmission and storage of classified

information on unclassified email systems and servers. The list of terms is subject to modification and is updated as necessary to reflect case developments.

III. Information To Be Seized by the Government

All information described above in Section I that constitutes evidence, contraband, fruits, and/or other items illegally possessed in violation of 18 U.S.C. § 793(e) and (f), those violations occurring from October 25, 2010 to December 31, 2010, including, for the SUBJECT ACCOUNT, information pertaining to the following matters:

a. Evidence indicating how and when the SUBJECT ACCOUNT was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the offenses under investigation and to the SUBJECT ACCOUNT owner;

b. The identity of the person(s) who communicated with the SUBJECT ACCOUNT about matters relating to the offenses under investigation, as described above.

IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

Alexandria Division

IN RE APPLICATION OF THE UNITED STATES OF AMERICA FOR AN ORDER PURSUANT TO 18 U.S.C. § 2703(d) TO GOOGLE, INC., AN INTERNET SERVICE PROVIDER	Misc. No. 1:16-ec-365 **Filed Under Seal**

APPLICATION OF THE UNITED STATES
FOR AN ORDER PURSUANT TO 18 U.S.C. § 2703(d)

The United States of America, moving by and through its undersigned counsel, respectfully submits under seal this *ex parte* application for an Order pursuant to 18 U.S.C. § 2703(d). The proposed Order would require Google, Inc., an Internet Service Provider located in Mountain View, CA, to disclose certain records and other information pertaining to the email account [redacted]@gmail.com. The records and other information to be disclosed are described in Attachment A to the proposed Order. In support of this application, the United States asserts:

LEGAL BACKGROUND

1. Google, Inc. is a provider of an electronic communications service, as defined in 18 U.S.C. § 2510(15), and/or a remote computing service, as defined in 18 U.S.C. § 2711(2). Accordingly, the United States may use a court order issued under § 2703(d) to require Google, Inc. to disclose the items described in Part II of Attachment A. *See* 18 U.S.C. § 2703(c)(2) (Part II.A of Attachment A); 18 U.S.C. § 2703(c)(1) (Part II.B of Attachment A).

2. This Court has jurisdiction to issue the proposed Order because it is "a court of competent jurisdiction," as defined in 18 U.S.C. § 2711. *See* 18 U.S.C. § 2703(d). Specifically,

the Court is a district court of the United States that has jurisdiction over the offense being investigated. *See* 18 U.S.C. § 2711(3)(A)(i).

3. A court order under § 2703(d) "shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d). Accordingly, the next section of this application sets forth specific and articulable facts showing that there are reasonable grounds to believe that the records and other information described in Part II of Attachment A are relevant and material to an ongoing criminal investigation.

THE RELEVANT FACTS

4. The government is conducting a criminal investigation concerning the improper transmission and storage of classified information on unclassified email systems and servers, in violation of Title 18, United States Code, Sections 793(e) and (f). The investigation began as a result of a review of emails undertaken by the U.S. Department of State in connection with Freedom of Information Act (FOIA) litigation. During this FOIA review, it was determined that certain emails containing classified information were sent and received on systems unauthorized for the transmission or storage of such information. On or about July 6, 2015, the Inspector General for the Intelligence Community notified the Federal Bureau of Investigation (FBI) of a potential compromise of classified information involving the emails discovered through the FOIA review. After an initial review of the matter, the FBI opened a criminal investigation to, among other things, identify any unauthorized systems which the emails in question have transited, identify any person(s) who may have introduced classified information onto

unauthorized systems and all circumstances surrounding such introduction, and identify any person(s) who may have transmitted such information over any such systems.

5. The FBI's investigation has established that the emails containing classified information have been transmitted and stored on multiple forms of electronic media. One of the items identified as having contained such emails is a server which was used by former Secretary of State Hillary Rodham Clinton ("Clinton") to transmit, receive, and store email for a personal email account or accounts she maintained. One domain on that server used by Clinton was @clintonemail.com.

6. Clinton's personal counsel, Williams & Connolly, LLP, voluntarily produced to the FBI, in a PST file,[1] over 30,000 emails sent to or from the @clintonemail.com domain, some of which have been confirmed to include information classified by the United States Government. During a review of these emails, the FBI discovered a large portion of emails carrying metadata displaying the email address [redacted]@gmail.com ("Subject Account"). According to subpoena returns from Google, the Subject Account is associated with Paul Combetta, who is an employee of Platte River Networks ("PRN"), a Denver, Colorado-based information technology firm that managed a server for Clinton beginning in June 2013.

7. In a recent interview, Combetta informed the FBI that he used the Subject Account to facilitate the transfer of Clinton archived emails to a PRN exchange server from a laptop belonging to a State Department staffer for the former Secretary. The FBI believes these archived emails included emails from the original dataset provided to the FBI by Williams & Connolly. In addition, as indicated above, the Subject Account appears in the metadata of the @clintonemail.com emails provided to the FBI by Williams & Connolly, which includes

[1] A PST (Personal Storage Table) file, often designated as .pst, is used to store Microsoft Outlook email messages and other data items on a local computer.

confirmed classified emails.

8. Based on the FBI's investigation, there is reason to believe that the Subject Account contains evidence related to the unlawful storage and transmission of classified information from the beginning of Clinton's tenure as Secretary of State on January 21, 2009, to the present.

REQUEST FOR ORDER

9. The facts set forth in the previous section show that there are reasonable grounds to believe that the records and other information described in Part II of Attachment A are relevant and material to an ongoing criminal investigation. Specifically, a review of these items for the time period January 21, 2009 to the present will help the FBI determine if any @clintonemail.com emails, including confirmed classified emails, from Clinton's tenure at the State Department, reside within the Subject Account. Accordingly, the United States requests that Google, Inc. be directed to produce all items described in Part II of Attachment A to the proposed Order.

10. The United States further requests that the Order require Google, Inc. not to notify any person, including the subscribers or customers of the account(s) listed in Part I of Attachment A, of the existence of the Order until further order of the Court. *See* 18 U.S.C. § 2705(b). This Court has authority under 18 U.S.C. § 2705(b) to issue "an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order." *Id.* In this case, such an order would be appropriate because the requested Order relates to an ongoing criminal investigation that is neither public nor known to all of the subjects of the investigation, and its

disclosure may alert subjects to the ongoing investigation. Accordingly, there is reason to believe that notification of the existence of the requested Order will seriously jeopardize the investigation, including by giving subjects an opportunity to destroy or tamper with evidence, or otherwise seriously jeopardize an ongoing investigation. *See* 18 U.S.C. § 2705(b)(3), (5). Because much of the evidence in this investigation is stored electronically, if alerted to the investigation, subjects could destroy that evidence, including information saved to personal computers.

11. The United States further requests that the Court order that this application and any resulting order be sealed until further order of the Court. As explained above, these documents discuss an ongoing criminal investigation that is neither public nor known to all of the subjects of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

Respectfully submitted,

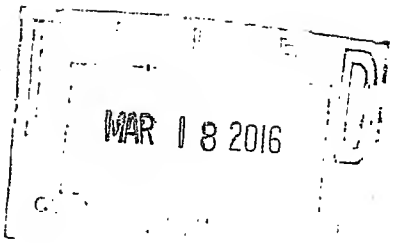
Dana J. Boente
United States Attorney

By: [redacted]
Assistant United States Attorney

IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

Alexandria Division



IN RE APPLICATION OF THE UNITED STATES OF AMERICA FOR AN ORDER PURSUANT TO 18 U.S.C. § 2703(d) TO GOOGLE, INC., AN INTENET SERVICE PROVIDER	)	Misc. No. 1:16-ec-365 **Filed Under Seal**

ORDER

The United States has submitted an application pursuant to 18 U.S.C. § 2703(d), requesting that the Court issue an Order requiring Google, Inc., an electronic communications service provider and/or a remote computing service located in Mountain View, CA, to disclose the records and other information described in Attachment A to this Order.

The Court finds that the United States has offered specific and articulable facts showing that there are reasonable grounds to believe that the records or other information sought are relevant and material to an ongoing criminal investigation.

The Court determines that there is reason to believe that notification of the existence of this Order will seriously jeopardize the ongoing investigation, including by giving subjects an opportunity to destroy or tamper with evidence, or otherwise seriously jeopardize an ongoing investigation. *See* 18 U.S.C. § 2705(b)(3), (5).

IT IS THEREFORE ORDERED, pursuant to 18 U.S.C. § 2703(d), that Google, Inc. shall, within ten days of the date of this Order, disclose to the United States the records and other information described in Attachment A to this Order.

IT IS FURTHER ORDERED that Google, Inc. shall not disclose the existence of the application of the United States, or the existence of this Order of the Court, to the subscriber(s) of the account listed in Attachment A, or to any other person, unless and until otherwise authorized to do so by the Court, except that Google, Inc. may disclose this Order to an attorney for Google, Inc. for the purpose of receiving legal advice.

IT IS FURTHER ORDERED that the application and this Order are sealed until otherwise ordered by the Court.

/s/
John F. Anderson
United States Magistrate Judge
John F. Anderson
United States Magistrate Judge

Date: March 18, 2016

At Alexandria, Virginia

A TRUE COPY, TESTE:
CLERK, U.S. DISTRICT COURT
BY
DEPUTY CLERK

ATTACHMENT A

I. The Account(s)

The Order applies to certain records and information associated with the following email account: [redacted]@gmail.com.

II. Records and Other Information to Be Disclosed

Google, Inc. is required to disclose the following records and other information, if available, to the United States for each account or identifier listed in Part I of this Attachment ("Account"), for the time period from January 21, 2009 to the present:

A. The following information about the customers or subscribers of the Account:

1. Names (including subscriber names, user names, and screen names);
2. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);
3. Local and long distance telephone connection records;
4. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions;
5. Length of service (including start date) and types of service utilized;
6. Telephone or instrument numbers (including MAC addresses);
7. Other subscriber numbers or identities (including the registration Internet Protocol ("IP") address); and
8. Means and source of payment for such service (including any credit card or bank account number) and billing records.

B. All records and other information (not including the contents of communications) relating to the Account, including:

1. Records of user activity for each connection made to or from the Account, including log files; messaging logs; the date, time, length, and method of connections; data transfer volume; user names; and source and destination Internet Protocol addresses;

2. Information about each communication sent or received by the Account, including the date and time of the communication, the method of communication, and the source and destination of the communication (such as source and destination email addresses, IP addresses, and telephone numbers).

CERTIFICATE OF AUTHENTICITY OF DOMESTIC BUSINESS RECORDS PURSUANT TO FEDERAL RULE OF EVIDENCE 902(11)

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Google, Inc., and my official title is _____. I am a custodian of records for Google, Inc.. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Google, Inc., and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;

b. such records were kept in the ordinary course of a regularly conducted business activity of Google, Inc.; and

c. such records were made by Google, Inc. as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

_____ _____

Date Signature